Derivations and I-smoothness

Swayam Chube

Last Updated: June 18, 2025

§1 Derivations

Definition 1.1. Let A be a ring and M an A-module. A *derivation* from A to M is a map $D\colon A \to M$ satisfying

(i) $D(a+b) = Da + Db$, and

(ii) $D(ab) = aDb + bDa$ for all $a, b \in A$.

The set of all such derivations is denoted by $\mathrm{Der}(A, M)$ and is naturally an A-module through

$$(D + D')a = Da + D'a \quad \text{and} \quad (aD)b = a(Db).$$

Further, if A is a k-algebra[1] via a ring homomorphism $f : k \to A$, we say that $D \in \mathrm{Der}(A, M)$ is a *k-derivation* if $D \circ f = 0$. The set of all k-derivations is denoted by $\mathrm{Der}_k(A, M)$.

For $D, D' \in \mathrm{Der}(A, M)$, define

$$[D, D'] = D \circ D' - D' \circ D \in \mathrm{Der}(A, M).$$

It is then easy to check that under the above bracket operation $\mathrm{Der}_k(A, M)$ forms a Lie algebra over k when k is a field.

Inductively, it is easy to show that derivations satisfy a "Leibnitz formula":

$$D^n(ab) = \sum_{i=0}^{n} \binom{n}{i} D^i a \cdot D^{n-i} b.$$

If A has characteristic $p > 0$, then we obtain

$$D^p(ab) = D^p a \cdot b + a \cdot D^p b,$$

so that $D^p \in \mathrm{Der}(A, M)$.

Note that the functor $\mathrm{Der}_k(A, -)\colon \mathfrak{Mod}_A \to \mathfrak{Mod}_A$ is covariant. We shall eventually show that it is "representable".

Remark 1.2. We remark that the k-derivations are precisely the k-linear derivations. Indeed, if $D \in \mathrm{Der}_k(A, M)$, then for $x \in k$ and $a \in A$, we have

$$D(xa) = xDa + aDx = xDa.$$

On the other hand, if $D \in \mathrm{Der}(A, M)$ is k-linear, then for $x \in k$, we have

$$Dx = D(x \cdot 1) = xD1 + Dx = Dx,$$

since

$$D1 = D(1 \cdot 1) = D1 + D1 \implies D1 = 0.$$

[1] k is any ring.

DEFINITION 1.3. Let A be a ring and N an A-module. We define the *idealization* of N in A to be

$$A \rtimes N := \left\{ \begin{pmatrix} a & x \\ & a \end{pmatrix} : a \in A,\ x \in N \right\}.$$

This clearly forms a ring under matrix multiplication. There is a natural map $A \to A \rtimes N$ embedding A as diagonal matrices and $N \hookrightarrow A \rtimes N$ sits as an ideal with $N^2 = 0$.

Let k be a ring and $k \to A$ a k-algebra. Let $\mu\colon A \otimes_k A \to A$ be given by $\mu(x \otimes y) = xy$, set $B := A \otimes_k A/I^2$ and $\Omega_{A/k} := I/I^2$. Since the annihilator of $\Omega_{A/k}$ as a B-module contains the ideal I, it is naturally an A-module. The action is explicitly given by

$$a \cdot (x \otimes y + I^2) = ax \otimes y + I^2 = x \otimes ay + I^2,$$

which is precisely the B-action through either $a \otimes 1 + I^2$ or $1 \otimes a + I^2$. Further, there is a natural map $d\colon A \to \Omega_{A/k}$ given by

$$da = 1 \otimes a - a \otimes 1.$$

It is easy to check that d is a k-derivation.

THEOREM 1.4. The pair $(\Omega_{A/k}, d)$ has the following universal property: If M is an A-module and $D \in \mathrm{Der}_k(A, M)$, then there is a unique A-linear map $f\colon \Omega_{A/k} \to M$ such that $f \circ d = D$.

In particular, there is a natural isomorphism of functors $\mathrm{Der}_k(A, -) \cong \mathrm{Hom}_A(\Omega_{A/k}, -)$.

Proof. Let $D \in \mathrm{Der}_k(A, M)$ and let $\varphi\colon A \otimes_k A \to A \rtimes M$ be given by

$$\varphi(x \otimes y) = \begin{pmatrix} xy & xDy \\ & xy \end{pmatrix}.$$

It is easy to check that φ is a homomorphism of k-algebras and φ maps I into M. Further, since $M^2 = 0$, it follows that $I^2 \subseteq \ker\varphi$, so that φ descends to a map $f\colon \Omega_{A/k} \to M$. This map is A-linear; indeed, if $\xi = \sum_i x_i \otimes y_i + I^2 \in \Omega_{A/k}$, then for $a \in A$,

$$f(a\xi) = \sum_i = ax_i y_i = af(\xi).$$

Moreover, for $a \in A$,

$$f(da) = f(1 \otimes a - a \otimes 1 + I^2) = Da,$$

so that $f\colon \Omega_{A/k} \to M$ is the desired map. To see that f is unique, it suffices to prove:

CLAIM. $\Omega_{A/k}$ is generated by $\{da : a \in A\}$ as an A-module.

Indeed, let $\xi = \sum_i x_i \otimes y_i + I^2 \in \Omega_{A/k}$. Then $\mu(\xi) = \sum_i x_i y_i = 0$, so that

$$\xi = \sum_i x_i (1 \otimes y_i - y_i \otimes 1) + \sum_i x_i y_i \otimes 1 = \sum_i x_i dy_i.$$

This completes the proof. ∎

PROPOSITION 1.5. Let A and k be k-algebras and set $A' = A \otimes_k k'$. Then

$$\Omega_{A'/k'} \cong \Omega_{A/k} \otimes_k k' \cong \Omega_{A/k} \otimes_A A'.$$

Proof. Let $d\colon A \to \Omega_{A/k}$ be the universal derivation. This induces a map $d' := d \otimes \mathbb{1}\colon A \otimes_k k' \to \Omega_{A/k} \otimes_k k'$. We claim that the tuple $(A', d', \Omega_{A/k} \otimes_k k')$ has the desired universal property. First, we must argue that d' is a k'-derivation. Indeed,

$$d'\big((a \otimes x) \cdot (a' \otimes x')\big) = d(aa') \otimes xx' = \big(ada' + a'da\big) \otimes xx' = (a \otimes x)d'(a' \otimes x') + (a' \otimes x')d'(a \otimes x),$$

and $d'(1 \otimes x) = d1 \otimes x = 0$ for all $x, x' \in k'$ and $a, a' \in A$. This shows that d' is a k'-derivation.

It remains to verify the universal property. Let $D'\colon A' \to M'$ be a k'-derivation. The composition $D\colon A \to A' \to M'$ is clearly a k-derivation, and hence there is an A-linear map $f\colon \Omega_{A/k} \to M'$ making

$$\begin{tikzcd} A \arrow[r, "D"] \arrow[d, "d"'] & M' \\ \Omega_{A/k} \arrow[ur, "f"'] & \end{tikzcd}$$

commute. The map f induces $f \otimes \mathbb{1}\colon \Omega_{A/k} \otimes_k k' \to M' \otimes_k k'$. There is a natural "multiplication" map $M' \otimes_k k' \to M'$ given by $m' \otimes x \mapsto x \cdot m'$. Denote g by the composition

$$g\colon \Omega_{A/k} \otimes_k k' \xrightarrow{f \otimes \mathbb{1}} M' \otimes_k k' \to M'.$$

We contend that g is A'-linear. Any element of A' is of the form $\sum_i a_i \otimes x_i$, so it suffices to check linearity for elements of the form $a \otimes x$ with $a \in A$ and $x \in k'$. Indeed, for $\omega \in \Omega_{A/k}$ and $x' \in k'$, we have

$$g\big((a \otimes x) \cdot (\omega \otimes x')\big) = f(a\omega) \otimes xx' = xx' \cdot f(a\omega) = (a \otimes x) \cdot (x' \cdot f(\omega)) = (a \otimes x) \cdot g(\omega \otimes x').$$

Finally, note that the diagram

$$\begin{tikzcd} A' \arrow[r, "D'"] \arrow[d, "d'"'] & M' \\ \Omega_{A/k} \otimes_k k' \arrow[ur, "g"'] & \end{tikzcd}$$

commutes because for $a \in A$ and $x \in k'$, we have

$$(g \circ d')(a \otimes x) = g(da \otimes x) = x \cdot f(da) = x \cdot Da = x \cdot D'(a \otimes 1) = D'(a \otimes x),$$

as desired. The uniqueness of g follows from the fact that $d'(A')$ generates $\Omega_{A/k} \otimes_k k'$ as an A'-module, and the commutativity of the diagram determines the value of g on the set $d'(A')$. This completes the proof. ■

Let A be a k-algebra, and $S \subseteq A$ be a multiplicative subset. If $D\colon A \to M$ is a k-derivation, then it induces a k-derivation $D_S\colon S^{-1}A \to S^{-1}M$ by

$$D\left(\frac{a}{s}\right) = \frac{s \cdot D(a) - a \cdot D(s)}{s^2} \in S^{-1}M.$$

It is an easy exercise to check that this is indeed a k-derivation.

PROPOSITION 1.6. Let A be a k-algebra, and $S \subseteq A$ a multiplicative subset. Then

$$\Omega_{S^{-1}A/k} \cong \Omega_{A/k} \otimes_A S^{-1}A = S^{-1}\Omega_{A/k}.$$

Proof. Let $d\colon A \to \Omega_{A/k}$ be the "universal derivation". We contend that the derivation $d_S\colon S^{-1}A \to S^{-1}\Omega_{A/k}$ has the desired universal property of Kähler differentials. Let M be an $S^{-1}A$-module and let $\partial\colon S^{-1}A \to M$ be a k-derivation. The composition $D\colon A \to S^{-1}A \to M$ is clearly a k-derivation, and hence induces an A-linear map $f\colon \Omega_{A/k} \to M$ making

$$\begin{tikzcd} A \arrow[r, "D"] \arrow[d, "d"'] & M \\ \Omega_{A/k} \arrow[ur, "f"'] & \end{tikzcd}$$

commute. The map f further induces an $S^{-1}A$-linear map $S^{-1}f\colon S^{-1}\Omega_{A/k} \to M$. We contend that the diagram

$$\begin{tikzcd} S^{-1}A \arrow[r, "\partial"] \arrow[d, "d_S"'] & M \\ S^{-1}\Omega_{A/k} \arrow[ur, "S^{-1}f"'] & \end{tikzcd}$$

commutes. Indeed,

$$S^{-1}f \circ d_S\left(\frac{a}{s}\right) = S^{-1}f\left(\frac{s\cdot da - a\cdot ds}{s^2}\right) = \frac{s\cdot f(da) - a\cdot f(ds)}{s^2} = \frac{s\cdot \partial a - a\cdot \partial s}{s^2} = \partial\left(\frac{a}{s}\right),$$

as desired. Again, the uniqueness follows from the fact that the image of $d_S(S^{-1}A)$ generates $S^{-1}\Omega_{A/k}$ as an $S^{-1}A$-module, thereby completing the proof. ∎

DEFINITION 1.7. Let k be a ring. We say that a k-algebra A is *0-smooth* if for any k-algebra C, any ideal $N \trianglelefteq C$ with $N^2 = 0$, and any k-algebra homomorphism $u\colon A \to C/N$, there exists a lift $v\colon A \to C$ making

$$\begin{tikzcd} k \arrow[r] \arrow[d] & C \arrow[d] \\ A \arrow[r, "u"'] \arrow[ur, dotted, "\exists\, v"] & C/N \end{tikzcd}$$

commute. Moreover, we say that A is *0-unramified* over k if there exists at most one such v. When A is both 0-smooth and 0-unramified, we say that A is *0-étale*.

LEMMA 1.8. Let $k \to A$ be a homomorphism of rings. Then A is 0-unramified over k if and only if $\Omega_{A/k} = 0$.

Proof. Indeed, suppose $\Omega_{A/k} = 0$, and there are two lifts

$$\begin{tikzcd} k \arrow[r] \arrow[d] & C \arrow[d, "\pi"] \\ A \arrow[r, "u"'] \arrow[ur, shift left, "\lambda_1"] \arrow[ur, shift right, "\lambda_2"'] & C/N. \end{tikzcd}$$

Let $D = \lambda_1 - \lambda_2\colon A \to N$. We note that N is naturally an A-module, through the action $a\cdot n = \pi^{-1}u(a)\cdot n$, which is well-defined since $N^2 = 0$. We claim that $D \in \mathrm{Der}_k(A,N)$. Let $a,b \in A$, then

$$\begin{aligned} aDb + bDa &= a\cdot(\lambda_1(b) - \lambda_2(b)) + b\cdot(\lambda_1(a) - \lambda_2(a)) \\ &= \lambda_1(a)(\lambda_1(b) - \lambda_2(b)) + \lambda_2(b)(\lambda_1(a) - \lambda_2(b)) \\ &= \lambda_1(ab) - \lambda_2(ab) \\ &= D(ab). \end{aligned}$$

But since $\Omega_{A/k} = 0$, we have $\mathrm{Der}_k(A,N) \cong \mathrm{Hom}_A(\Omega_{A/k}, N) = 0$, whence $D = 0$, and thus $\lambda_1 = \lambda_2$.

Conversely, suppose A is 0-unramified over k. Consider the commutative diagram

$$\begin{tikzcd} k \arrow[r] \arrow[d] & A \otimes_k A/I^2 \arrow[d] \\ A \arrow[r] & A \otimes_k A/I \end{tikzcd}$$

where $I = \ker\left(\mu\colon A \otimes_k A \to A\right)$ and the bottom map is $a \mapsto a \otimes 1$. Let $\lambda_1\colon A \to A \otimes_k A/I^2$ and $\lambda_2\colon A \to A \otimes_k A/I^2$ be given by

$$\lambda_1(a) = 1 \otimes a + I^2 \quad \text{ and } \lambda_2(a) = a \otimes 1 + I^2.$$

These are both lifts of the bottom map and hence must be equal. That is, $da = 1 \otimes a - a \otimes 1 \in I^2$. Since the da's generate $\Omega_{A/k}$ as an A-module, we must have that $\Omega_{A/k} = 0$, as desired. ∎

THEOREM 1.9 (FIRST FUNDAMENTAL EXACT SEQUENCE). Let $k \xrightarrow{f} A \xrightarrow{g} B$ be ring homomorphisms. This gives rise to an exact sequence

$$\Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \to 0, \tag{1}$$

where the maps are given by

$$\alpha(d_{A/k}a \otimes b) = b d_{B/k} g(a) \quad \text{and } \beta(d_{B/k}b) = d_{B/A}b.$$

If moreover B is 0-smooth over A, then the sequence

$$0 \to \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \xrightarrow{\beta} \Omega_{B/A} \to 0, \tag{2}$$

is split exact.

Proof. Let T be a B-module. To show that (1) is exact, it suffices to show that

$$0 \to \mathrm{Hom}_B(\Omega_{B/A}, T) \xrightarrow{\beta^*} \mathrm{Hom}_B(\Omega_{B/k}, T) \xrightarrow{\alpha^*} \mathrm{Hom}_B(\Omega_{A/k} \otimes_A B, T).$$

Using the Hom-Tensor adjunction, we have

$$\mathrm{Hom}_B(\Omega_{A/k} \otimes_A B, T) \cong \mathrm{Hom}_B(B, \mathrm{Hom}_A(\Omega_{A/k}, T)) \cong \mathrm{Hom}_A(\Omega_{A/k}, T) \cong \mathrm{Der}_k(A, T).$$

Thus, it suffices to show that

$$0 \to \mathrm{Der}_A(B, T) \xrightarrow{\text{inclusion}} \mathrm{Der}_k(B, T) \xrightarrow{-\circ g} \mathrm{Der}_k(A, T)$$

is exact. Indeed, if $D \in \mathrm{Der}_k(B, T)$ is such that $D \circ g = 0$, then D is an A-derivation, i.e., it lies in $\mathrm{Der}_A(B, T)$.

Suppose now that B is 0-smooth over A and let $D \in \mathrm{Der}_k(A, T)$. Consider the commutative diagram

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "g"'] & B \ltimes T \arrow[d] \\ B \arrow[r, equal] & B \end{tikzcd}$$

where

$$\varphi(a) = \begin{pmatrix} g(a) & Da \\ & g(a) \end{pmatrix}.$$

Due to smoothness, there is a lift $\psi : B \to B \ltimes T$ which can be written as

$$\psi(b) = \begin{pmatrix} b & D'b \\ & b \end{pmatrix}.$$

It is clear that $D' \in \mathrm{Der}_k(B, T)$. Further, $D' \circ g = D$ since $\psi \circ g = \varphi$. This shows that $-\circ g$ is a surjective map.

Now note that D' corresponds to a B-linear $\alpha' : \Omega_{B/k} \to T$. Take $T := \Omega_{A/k} \otimes B$ and define D by $Da = d_{A/k}a \otimes 1$, so that $D = D' \circ g$ implies $\alpha' \circ \alpha = \mathbf{id}_{\Omega_{A/k} \otimes_A B}$, as desired. ∎

THEOREM 1.10 (SECOND FUMDAMENTAL EXACT SEQUENCE). Let $k \xrightarrow{f} A \xrightarrow{g} B$ be ring homomorphisms with g surjective[2] and set $\mathfrak{a} := \ker g$. There is an exact sequence

$$\mathfrak{a}/\mathfrak{a}^2 \xrightarrow{\delta} \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \to 0, \tag{3}$$

where $\delta(x + \mathfrak{m}^2) = d_{A/k}x \otimes 1$. If moreover B is 0-smooth over k, then

$$0 \to \mathfrak{a}/\mathfrak{a}^2 \xrightarrow{\delta} \Omega_{A/k} \otimes_A B \xrightarrow{\alpha} \Omega_{B/k} \to 0 \tag{4}$$

is a split exact sequence.

[2]Clearly, this implies that $\Omega_{B/A} = 0$, for if $D \in \mathrm{Der}_A(B, M)$, then $D \circ g = 0$, i.e., $D = 0$ due to the surjectivity of g. The point of Theorem 1.10 is to characterize the kernel of the map $\Omega_{A/k} \otimes_A B \to \Omega_{B/k}$.

Proof. The surjectivity of α has been argued in the footnote. We shall show exactness at $\Omega_{A/k} \otimes_A B$. Again, let T be a B-module. It suffices to show that the sequence

$$\mathrm{Hom}_B(\Omega_{B/k}, T) \xrightarrow{\alpha^*} \mathrm{Hom}_B(\Omega_{A/k} \otimes_A B, T) \xrightarrow{\delta^*} \mathrm{Hom}_B(\mathfrak{a}/\mathfrak{a}^2, T)$$

is exact. Using the Hom-Tensor adjunction and Theorem 1.4, the above is isomorphic to the sequence

$$\mathrm{Der}_k(B,T) \xrightarrow{-\circ g} \mathrm{Der}_k(A,T) \xrightarrow{\delta^*} \mathrm{Hom}_B(\mathfrak{a}/\mathfrak{a}^2, T).$$

Note that for $a, b \in \mathfrak{a}$, $D(ab) = aD(b) + bD(a) = 0$ since $\mathfrak{a}$ acts trivially on T as the latter is a $B = A/\mathfrak{a}$-module. This shows that every $D \in \mathrm{Der}_k(A,T)$ descends to a map $\delta^* D \colon \mathfrak{a}/\mathfrak{a}^2 \to T$ given by

$$\delta^* D(a + \mathfrak{a}^2) = Da.$$

To see that this map is B-linear, let $b + \mathfrak{a} \in B$ and $a + \mathfrak{a}^2 \in \mathfrak{a}/\mathfrak{a}^2$. Then

$$\delta^* D\left(ab + \mathfrak{a}^2\right) = aDb + bDa = bDa,$$

thereby proving that $\delta^* D$ is B-linear.

Now, $\delta^* D = 0$ if and only if $D(\mathfrak{m}) = 0$, so that D can be lifted to a k-derivation $B \to T$, whence (3) is exact.

Suppose now that B is 0-smooth over k. Then there is a lift

$$\begin{tikzcd} k \arrow[r] \arrow[d] & A/\mathfrak{m}^2 \arrow[d, "g"] \\ B \arrow[r, equal] \arrow[ur, dotted, "\exists"] & B \end{tikzcd}$$

so that the short exact sequence

$$0 \to \mathfrak{m}/\mathfrak{m}^2 \to A/\mathfrak{m}^2 \xrightarrow{g} B \to 0$$

splits, i.e., there exists a homomorphism of k-algebras $s \colon B \to A/\mathfrak{m}^2$ such that $g \circ s = \mathbf{id}_B$. Now, $sg \colon A/\mathfrak{m}^2 \to A/\mathfrak{m}^2$ is a homomorphism vanishing on $\mathfrak{m}/\mathfrak{m}^2$, and $g = \mathbf{id}_B \circ g = gsg$, i.e., $g(1 - sg) = 0$. Set $D = 1 - sg$, then $D \colon A/\mathfrak{m}^2 \to \ker g = \mathfrak{m}/\mathfrak{m}^2$ is a derivation. Indeed, if $a, b \in A$, then

$$D(ab + \mathfrak{m}^2) = (ab + \mathfrak{m}^2) -$$

■

THEOREM 1.11. Suppose L/K is a separable algebraic extension of fields. Then L is 0-étale over K. Moreover, for any subfield $k \subseteq K$, we have

$$\Omega_{L/k} = \Omega_{K/k} \otimes_K L.$$

Proof. Let C be a K-algebra with an ideal $N \trianglelefteq C$ such that $N^2 = 0$, and let $u \colon L \to C/N$ be a K-algebra homomorphism.

$$\begin{tikzcd} K \arrow[r] \arrow[d] & C \arrow[d, "\pi"] \\ L \arrow[r, "u"'] & C/N \end{tikzcd}$$

Let L' be an intermediate field $K \subseteq L' \subseteq L$ with L' finite over K. Using the Primitive Element Theorem, we can write $L' = K(\alpha)$ for some $\alpha \in L'$. Let $f(X) \in K[X]$ be the minimal polynomial of α over K, so that $L' \cong K[X]/(f(X))$ and $f'(\alpha) \neq 0$. We shall first lift $u|_{L'} \colon L' \to C/N$ to a map $L' \to C$. This is equivalent to finding an element $y \in C$ satisfying $f(y) = 0$, and $\pi(y) = u(\alpha)$.

Choose any inverse image $y \in C$ of $u(\alpha)$. Then $\pi(f(y)) = u(f(\alpha)) = 0$, so that $f(y) \in N$. Moreover, $N^2 = 0$, so for any $\eta \in N$, using Taylor's expansion, we get

$$f(y + \eta) = f(y) + f'(y)\eta.$$

Recall that $f'(\alpha)$ is a unit in L, so that $u(f'(\alpha)) = \pi(f'(y))$ is a unit in C/N, whence $f'(y)$ is a unit in C[3]. Set $\eta = -f(y)/f'(y) \in N$, and $f(y+\eta) = 0$. Let $v\colon L' \to C$ be obtained by sending $\alpha \mapsto y+\eta$. Clearly this is a lifting of $u|_{L'}\colon L' \to C/N$.

$$\begin{tikzcd} K \arrow[r] \arrow[d] & C \arrow[d, "\pi"] \\ L' \arrow[r, "u|_{L'}"'] & C/N \end{tikzcd}$$

We claim that this lift is unique. Indeed, suppose there are two lifts $v\colon \alpha \mapsto y$ and $\widetilde{v}\colon \alpha \mapsto \widetilde{y}+\eta$. Then, using the formula $f(y+\eta) = f(y) + f'(y)\eta$, and the facts that $f(y+\eta) = f(y) = 0$, we note that $f'(y)\eta = 0$. But as we have argued previously, $f'(y)$ is a unit in C, whence $\eta = 0$, as desired.

Thus for every $\alpha \in L$, there is a uniquely determined lifting $v_\alpha\colon K(\alpha) \to C$ of $u|_{K(\alpha)}\colon K(\alpha) \to C$. Now define $v\colon L \to C$ by $v(\alpha) = v_\alpha(\alpha)$ for all $\alpha \in L$. To see that v is a K-algebra homomorphism, note that for $\alpha, \beta \in L$, there is a $\gamma \in L$ such that $K(\alpha,\beta) = K(\gamma)$. Further, due to the uniqueness of intermediate lifts as argued in the preceding paragraph, we must have that $v_\gamma|_{K(\alpha)} = v_\alpha$ and $v_\gamma|_{K(\beta)} = v_\beta$, whence it follows that v is a K-algebra homomorphism. That v is a lift is clear since it is a lift when restricted to finite intermediate extensions.

The last assertion follows from Theorem 1.9 since we have a short exact sequence

$$0 \to \Omega_{K/k} \otimes_K L \to \Omega_{L/k} \to \Omega_{L/K} \to 0,$$

and $\Omega_{L/K} = 0$ due to Lemma 1.8. ■

Remark 1.12. It is important to know what the above isomorphism exactly is. Recall the map $\alpha\colon \Omega_{K/k} \otimes_K L \to \Omega_{L/k}$ from Theorem 1.9; $\alpha(d_{K/k}a \otimes b) = b\, d_{L/k}a$. Identify $\Omega_{K/k}$ with the K-subspace generated by the image of $\{dx \otimes 1\colon x \in K\}$ under α. According to our isomorphism, a K-basis of this subspace constitutes an L-basis of $\Omega_{L/k}$.

We claim that any $D \in \mathrm{Der}_k(K)$ can be extended to a k-linear derivation of L. Indeed, corresponding to this derivation there is a unique K-linear map $f\colon \Omega_{K/k} \to K$ such that $D = f \circ d_{K/k}$. Under the identification made above, the map f extends to a unique L-linear map $F\colon \Omega_{L/k} \to L$. Then it is clear that $\widetilde{D} = F \circ d_{L/k} \in \mathrm{Der}_k(L)$ is a derivation extending D.

§2 Separability

Definition 2.1. Let k be a field and A a k-algebra. We say that A is *separable* over k if for every field extension $k \subseteq k'$, the ring $A' = A \otimes_k k'$ is reduced.

From the definition, the following properties are evident:

(i) A subalgebra of a separable k-algebra is separable.

(ii) A is separable over k if and only if every finitely generated k-subalgebra of A is separable over k.

(iii) For A to be separable over k, it is sufficient that $A \otimes_k k'$ is reduced for every finitely generated extension field k' of k.

(iv) If A is separable over k, and k' is an extension field of k, then $A \otimes_k k'$ is separable over k'.

Property (i) is trivial since for any subalgebra $B \subseteq A$, the map $B \otimes_k k' \to A \otimes_k k'$ is an injective ring homomorphism. To see (ii) and (iii), suppose $\xi = \sum_{i=1}^n a_i \otimes b_i$ is nilpotent in $A \otimes_k k'$, then it is nilpotent in $B \otimes_k \ell$, where $B = k[a_1, \ldots, a_n]$, and $\ell = k(b_1, \ldots, b_n)$. Finally, to see (iv), note that for any field extension $k' \subseteq \ell$,

$$\left(A \otimes_k k'\right) \otimes_{k'} \ell = A \otimes_k \left(k' \otimes_{k'} \ell\right) = A \otimes_k \ell,$$

which is reduced since A is separable over k.

[3]In general, if R is a ring and I a nilpotent ideal, then any element congruent to a unit modulo I is a unit in R. This follows from the fact that the nilradical is the intersection of all prime ideals, and that every non-unit in R is contained in a (prime) maximal ideal.

Remark 2.2. We note that the above definition of separability is an extension of the usual definition encountered in field theory. Indeed, let $K \supseteq k$ be a separable algebraic extension. To verify that K is a separable k-algebra, using property (ii) above, we may assume that K is finitely generated over k. Using the Primitive Element Theorem, there is an isomorphism $K \cong k[X]/(f(X))$ for some irreducible separable polynomial $f(X) \in k[X]$.

If $k' \supseteq k$ is a field extension, then due to the Chinese Remainder Theorem,

$$K \otimes_k k' \cong k'[X]/(f(X)) \cong \prod_{i=1}^{n} k[X]/(f_i(X)),$$

where $f(X) = f_1(X)\cdots f_n(X)$ is the decomposition of $f(X)$ into irreducibles in $k[X]$. Note that $f_i \neq f_j$ for $1 \leqslant i < j \leqslant n$ since $f(X)$ has no multiple roots in any algebraically closed field containing k, in particular, $\overline{k'}$. This shows that $K \otimes_k k'$ is reduced, as desired.

Definition 2.3. A field extension $k \subseteq K$ is said to be *separably generated* if there is a transcendence basis Γ of the extension such that $K/k(\Gamma)$ is a separable algebraic extension.

Theorem 2.4. If $k \subseteq K$ is a separably generated field extension, then K is a separable algebra over k.

Proof. Let $\Gamma \subseteq K$ be a separating transcendence basis over k, that is, $K/k(\Gamma)$ is a separable algebraic extension. If $k' \supseteq k$ is an extension of fields, then $k(\Gamma) \otimes_k k'$ is a localization of $k[\Gamma] \otimes_k k' \cong k'[\Gamma]$, whence the former is an integral domain with field of fractions isomorphic to $k'(\Gamma)$ as a k-algebra. Therefore,

$$K \otimes_k k' \cong \left(K \otimes_{k(\Gamma)} k(\Gamma)\right) \otimes_k k' \cong K \otimes_{k(\Gamma)} \left(k(\Gamma) \otimes_k k'\right) \hookrightarrow K \otimes_{k(\Gamma)} k'(\Gamma).$$

Due to Remark 2.2, $K \otimes_{k(\Gamma)} k'(\Gamma)$ is reduced, and hence so is $K \otimes_k k'$, as desired. ■

Theorem 2.5. Let k be a field of characteristic $p > 0$, and K a finitely generated extension field of k. The following are equivalent:

(1) K is a separable algebra over k.

(2) $K \otimes_k k^{1/p}$ is reduced.

(3) K is separably generated over k.

Proof. The implication (1) $\implies$ (2) is clear and (3) $\implies$ (1) is the content of Theorem 2.4. We shall prove (2) $\implies$ (3). Let $K = k(x_1, \ldots, x_n)$, we can further arrange that $x_1, \ldots, x_r$ is a transcendence basis for K over k. Suppose further that $x_{r+1}, \ldots, x_q$ are separably algebraic over $k(x_1, \ldots, x_r)$, and that x_{q+1} is not. Set $y = x_{q+1}$ so that the minimal polynomial of y over $k(x_1, \ldots, x_r)$ is of the form $f(Y^p)$ for some $f(Y) \in k(x_1, \ldots, x_r)[Y]$. Clearing denominators and using the fact that $x_1, \ldots, x_r$ are algebraically independent, we obtain an irreducible polynomial $F(X_1, \ldots, X_r, Y^p) \in k[X_1, \ldots, X_r, Y]$ with $F(x_1, \ldots, x_r, y^p) = 0$.

Now if all partial derivatives $\partial F/\partial X_i$ are identically zero, then $F(X_1, \ldots, X_r, Y^p)$ is the p-th power of a polynomial $G(X_1, \ldots, X_r, Y) \in k^{1/p}[X_1, \ldots, X_r, Y]$. But then we would have

$$k[x_1, \ldots, x_r, y] \otimes_k k^{1/p} = \left(\frac{k[X_1, \ldots, X_r, Y]}{F(X, Y^p)}\right) \otimes_k k^{1/p} = \frac{k^{1/p}[X_1, \ldots, X_r, Y]}{G(X, Y)^p},$$

which is a non-reduced subring of $K \otimes_k k^{1/p}$, a contradiction. Thus, we may suppose without loss of generality that $\partial F/\partial X_1 \neq 0$. Then x_1 is separably algebraic over $k(x_2, \ldots, x_r, y)$. Due to transitivity of (algebraic) separability, it follows that $x_{r+1}, \ldots, x_q$ are separable over $k(x_2, \ldots, x_r, y)$. Now set $\widetilde{x}_1 = y$ and $\widetilde{x}_{q+1} = x_1$. Then $\widetilde{x}_1, x_2, \ldots, x_r$ forms a transcendence basis of K/k and $x_{r+1}, \ldots, \widetilde{x}_{q+1}$ are separably algebraic over $k(\widetilde{x}_1, x_2, \ldots, x_r)$. Iterating this process, it is clear that we obtain a separating transcendence basis of K/k. ■

Porism 2.6. It follows from the proof that if $K = k(x_1, \ldots, x_n)$ is separable over k, then we can choose a separating transcendence basis contained in $\{x_1, \ldots, x_n\}$.

INTERLUDE 2.7 (AN ALTERNATE CHARACTERIZATION OF SEPARABILITY FOR FIELDS). The following definition can be found in [Sta18, Tag 030I]:

> An extension of fields $k \subseteq K$ is said to be *separable* if for every subextension $k \subseteq K' \subseteq K$ with K' a finitely generated field extension of k, the extension $k \subseteq K'$ is separably generated, that is, there is a transcendence basis $\Gamma \subseteq K'$ such that $k(\Gamma) \subseteq K'$ is a separable algebraic extension.

We remark here that the above definition is equivalent to ours. Indeed, suppose $k \subseteq K$ is an extension of fields which is separable in the sense of Definition 2.1. Suppose first that $\operatorname{char} k = p > 0$. As we remarked earlier, K is a separable k-algebra if and only if every finitely generated subextension $k \subseteq K' \subseteq K$ is a separable k-algebra, which in view of Theorem 2.5 happens if and only if it is separably generated over k, if and only if $k \subseteq K$ is a separable extension of fields in the sense of [Sta18, Tag 030I].

Next, if $\operatorname{char} k = 0$, then every $k \subseteq K$ is clearly a separable extension in the sense of [Sta18, Tag 030I]. On the other hand, K is a separable k-algebra if and only if every finitely generated subextension $k \subseteq K' \subseteq K$ is a separable k-algebra, which is true in view of Theorem 2.4. This establishes the equivalence of the two definitions in the case of field extensions.

THEOREM 2.8. Let k be a perfect field.

(1) Every field extension of k is separable.

(2) A k-algebra is separable if and only if it is reduced.

Proof. (1) Let K/k be an extension of fields. Note that in characteristic 0 every extension is separably generated, and therefore, every extension is separable. Suppose now that $\operatorname{char} k = p > 0$. In this case, k being perfect is equivalent to $k = k^{1/p}$. In view of Theorem 2.5, it follows that every finitely generated subextension of K/k is a separable k-algebra, whence K is a separable k-algebra.

(2) Clearly every separable k-algebra must be reduced. Conversely, suppose A is a reduced k-algebra. We may suppose without loss of generality that A is finitely generated, and hence, Noetherian. Let $\mathfrak{A}$ denote the total ring of fractions of A. The map $A \to \mathfrak{A}$ is an inclusion of k-algebras, therefore it suffices to show that $\mathfrak{A}$ is reduced. Recall that the total ring of fractions of a Noetherian reduced ring is Artinian, whence is a (finite) product of Artinian local rings. Since a reduced Artinian ring is a field, it follows that $\mathfrak{A}$ is a finite product of fields, say $\mathfrak{A} = K_1 \times \dots K_n$. Since k is perfect, each K_i is a separable k-algebra, so that $\mathfrak{A}$ is a separable k-algebra, whence so is A, being isomorphic to a subalgebra of $\mathfrak{A}$. This completes the proof. ■

LEMMA 2.9. Let K and K' be two subfields of a larger field L and let k be a common subfield contained in $K \cap K'$. The following conditions are equivalent:

(1) if $\alpha_1, \dots, \alpha_n \in K$ are linearly independent over k, then they are also linearly independent over K'.

(2) if $\alpha_1, \dots, \alpha_n \in K'$ are linearly independent over k, then they are also linearly independent over K.

(3) The natural multiplication map $K \otimes_k K' \to K[K'] = K'[K]$ is an isomorphism of k-algebras.

In this case K and K' are said to be *linearly disjoint* over k.

Proof. (1) $\Longrightarrow$ (3) Let $\xi = \sum_i x_i \otimes y_i$ be an element in the kernel of the multiplication map. We may suppose that the x_i's are linearly independent over k. Then $\sum_i y_i x_i = 0$, but according to (1), the x_i's are linearly independent over K', so that $y_i = 0$ for all i, i.e., $\xi = 0$. Thus the multiplication map is injective. Its surjectivity is clear, and hence it is an isomorphism.

(3) $\Longrightarrow$ (1) Suppose $\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n = 0$ for some $\lambda_1, \dots, \lambda_n \in K'$. Then $\sum_{i=1}^n \alpha_i \otimes \lambda_i$ lies in the kernel of the multiplication map, which is zero, whence $\lambda_i = 0$ for each $1 \leqslant i \leqslant n$.

Since the assertion (3) is symmetric in K and K', the equivalence of the three statements follows. ■

THEOREM 2.10 (MACLANE). Let k be a field of characteristic $p > 0$, and let K be a field extension of k. Fix an algebraic closure $\overline{K}$ containing K, and set

$$k^{p^{-n}} = \left\{\alpha \in \overline{K} \colon \alpha^{p^n} \in k\right\} \quad \text{and } k^{p^{-\infty}} = \bigcup_{n \geqslant 1} k^{p^{-n}}.$$

(1) If K is a separable k-algebra, then K and $k^{p^{-\infty}}$ are linearly disjoint over k.

(2) If K and $k^{p^{-n}}$ are linearly disjoint over k for some $n \geqslant 1$, then K is a separable k-algebra.

Proof. (1) Let $\alpha_1, \dots, \alpha_n \in K$ be linearly independent over k. Suppose $\lambda_1, \dots, \lambda_n \in k^{p^{-\infty}}$ are such that $\lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n = 0$. There is a positive integer $m > 0$ such that $\lambda_i^{p^m} \in k$ for each $1 \leqslant i \leqslant n$. Set $k_1 = k(\lambda_1, \dots, \lambda_n)$ and $A = K \otimes_k k_1$. Since A is a finite-dimensional K-vector space, it must be Artinian. Further, for each $a \in A$, $a^{p^m} \in K$, consequently, A must be a local ring. Since A is reduced, it has to be a field. Thus the multiplication map $A \to K[k_1]$ must be injective, so an isomorphism. The conclusion follows.

(2) If K and $k^{p^{-n}}$ are linearly disjoint over k, then since $k^{p^{-1}} \subseteq k^{p^{-n}}$, it follows that K and $k^{p^{-1}}$ are linearly disjoint over k. Let K' be a finitely generated subfield of K over k. Note that $K' \otimes_k k^{p^{-1}}$ is a subring of $K \otimes k^{p^{-1}} = K[k^{p^{-1}}]$, so that the former is reduced. In view of Theorem 2.5, K' is a separable k-algebra, whence so is K. ■

Here's a lemma about "base change" and linear disjointness which we shall require later:

Lemma 2.11. Let L be a large field containing subfields $k \subseteq k' \subseteq K$ and $k \subseteq K'$. Suppose K and K' are linearly disjoint over k. Then

(1) $K \cap K' = k$, and

(2) K and $k'(K')$ are linearly disjoint over k'.

$$\begin{tikzcd}
K & K'(k') \\
k' \arrow[u, dash] \arrow[ur, dash] & K' \arrow[u, dash] \\
k \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

§§ Differential Bases

Let $k \subseteq K$ be an extension of fields. Then $\Omega_{K/k}$ is a K-vector space spanned by the set $\{dx : x \in K\}$.

Definition 2.12. A subset $B \subseteq K$ such that $\{dx : x \in B\}$ forms a K-basis of $\Omega_{K/k}$ is called a *differential basis* for the field extension $k \subseteq K$.

Theorem 2.13. If $\operatorname{char} k = 0$, then the notion of a differential basis for $k \subseteq K$ coincides with the notion of a transcendence basis.

Proof. We first show that the linear independence of $dx_1, \dots, dx_n \in \Omega_{K/k}$ is equivalent to the K-linear independence of $x_1, \dots, x_n \in K$. Indeed, suppose first that $dx_1, \dots, dx_n$ are K-linearly independent. If $0 \neq f(X_1, \dots, X_n) \in k[X_1, \dots, X_n]$ is such that $f(x_1, \dots, x_n) = 0$, then choosing f of the smallest possible degree, we have

$$0 = df(x_1, \dots, x_n) = \sum_{i=1}^{n} f_i(x_1, \dots, x_n)dx_i,$$

where $f_i(X_1, \dots, X_n) = \frac{\partial}{\partial X_i} f(X_1, \dots, X_n)$. The minimality of the degree of f forces at least one of the coefficients $f_i(x_1, \dots, x_n) \neq 0$, which is a contradiction to linear independence.

Conversely, suppose $B = \{x_1, \dots, x_n\}$ are algebraically independent over k. There are k-linear derivations $D_i = \frac{\partial}{\partial x_i}$ of $k(B)$. Note that $K/k(B)$ is separable, and hence, in view of Remark 1.12, these derivations can be extended to k-linear derivations of K with the property that $D_i(x_j) = \delta_{i,j}$. Each derivation corresponds to a K-linear map $f_i : \Omega_{K/k} \to K$ such that $f_i \circ d = D_i$. It is now immediate that the differentials $dx_1, \dots, dx_n \in \Omega_{K/k}$ must be K-linearly independent. ■

Definition 2.14. Let $\operatorname{char} k = p > 0$. We say that $x_1, \ldots, x_n \in K$ are *p-independent* over k if

$$[K^p(k, x_1, \ldots, x_n) : K^p(k)] = p^n.$$

A subset $B \subseteq K$ is said to be p-independent if every finite subset of B is p-independent.

Suppose $x_1, \ldots, x_n \in K$ are p-independent. Then there is a tower of field extensions

$$K^p(k) \subseteq K^p(k, x_1) \subseteq \cdots \subseteq K^p(k, x_1, \ldots, x_n).$$

Further, since $x_i^p \in K^p$ for all $1 \leqslant i \leqslant n$, we have

$$[K^p(k, x_1, \ldots, x_i) : K^p(k, x_1, \ldots, x_{i-1})] \leqslant p,$$

hence, we have that $[K^p(k, x_1, \ldots, x_i) : K^p(k, x_1, \ldots, x_{i-1})] = p$ for $1 \leqslant i \leqslant n$. The converse statement is clearly true. It follows that $B \subseteq K$ is p-independent if and only if

$$\Gamma_B := \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} : x_1, \ldots, x_n \in B \text{ are distinct and } 0 \leqslant \alpha_i < p\}$$

is linearly independent over $K^p(k)$.

Definition 2.15. A subset $B \subseteq K$ is said to be a *p-basis* if it is p-independent and $K = K^p(k, B)$.

It clear from the characterization of p-independence as in (2.1) and a standard application of Zorn's lemma that every p-independent subset of K is contained in a p-basis of K over k. Further, $B \subseteq K$ is a p-basis over k if and only if Γ_B is a $K^p(k)$-basis of K.

Theorem 2.16. If $\operatorname{char} k = p > 0$, then the notion of a differential basis for $k \subseteq K$ coincides with the notion of a p-basis.

Proof. Suppose first that $B \subseteq K$ is a p-basis over k. Then any map $D : B \to K$ can be extended to a derivation in $\operatorname{Der}_k(K)$ by defining it on monomials in Γ_B as

$$D(x_1^{\alpha_1} \cdots x_n^{\alpha_n}) = \sum_{i=1}^{n} \alpha_i x_1^{\alpha_1} \cdots x_i^{\alpha_i - 1} \cdots x_n^{\alpha_n} D(x_i),$$

and extending $K^p(k)$-linearly. This is clearly a derivation since every element in K can be uniquely written as a $K^p(k)$-linear combination of elements from Γ_B. The uniqueness of such a derivation follows from the fact that any $D \in \operatorname{Der}_k(K)$ must vanish on $K^p(k)$, whence it must be $K^p(k)$-linear.

Conversely, suppose B is a differential basis of $k \subseteq K$. We claim that B is p-independent over k, suppose not, then there exist $x_1, \ldots, x_n \in B$ such that $x_1 \in K^p(k, x_2, \ldots, x_n)$. Hence, we can choose a polynomial $f(X_2, \ldots, X_n) \in K^p(k)[X_2, \ldots, X_n]$ such that $x_1 = f(x_2, \ldots, x_n)$. Passing to $\Omega_{K/k}$, we see that

$$dx_1 = \sum_{i=2}^{n} \frac{\partial f}{\partial X_i}(x_2, \ldots, x_n) dx_i,$$

a contradiction to the fact that B is a differential basis. Hence B must be p-independent, and as such, is contained in a p-basis $\widetilde{B}$ of K over k. As we have shown in the first paragraph, $\widetilde{B}$ must form a differential basis, therefore, $B = \widetilde{B}$, whence B forms a p-basis of K over k. This completes the proof. ∎

For a field k, let $\Pi \subseteq k$ denote the prime subfield. We use the shorthand Ω_k for the k-module $\Omega_{k/\Pi}$.

Theorem 2.17. For a field extension K/k, the following are equivalent:

(1) K/k is separable.

(2) for any subfield $k' \subseteq k$, the map $\alpha : \Omega_{k/k'} \otimes_k K \to \Omega_{K/k'}$ is injective.

(3) for any subfield $k' \subseteq K$ and any differential basis of k/k', there exists a differential basis of K/k' containing B.

(4) $\Omega_k \otimes_k K \to \Omega_k$ is injective.

(5) any derivation of k to an arbitrary k-module M extends to a derivation from K to M.

Proof. The equivalence of (2) and (3) is clear, for details try to mimic the argument in Remark 1.12, from which the implication (2) $\implies$ (4) $\iff$ (5) is also clear.

(1) $\implies$ (3) In characteristic 0, since the notion of a differential basis corresponds with that of a transcendence basis, there's no implication to prove since both (1) and (3) are true. Suppow now that $\operatorname{char} k = p > 0$. Due to Theorem 2.10, K and $k^{1/p}$ are linearly disjoint over k. Since $x \mapsto x^p$ is a field homomorphism, it follows that K^p and k are linearly disjoint over k^p. Using Lemma 2.11, it follows that $K^p(k^p, k') = K^p(k')$ and k are linearly disjoint over $k^p(k')$.

$$\begin{tikzcd}
k \arrow[d, dash] & K(k^p, k') \arrow[dl, dash] \arrow[d, dash] \\
k^p(k') \arrow[d, dash] & K \arrow[dl, dash] \\
k^p &
\end{tikzcd}$$

Choose a p-basis B of k over k', then the set Γ_B is $k^p(k')$-linearly independent, whence due to linear disjointness, is also $K^p(k')$-linearly independent. Thus B as a subset of K is also p-independent over k', whence it can be extended to a p-basis of K over k' and (3) follows.

(4) $\implies$ (1) Again, there's nothing to prove in characteristic zero. Suppose $\operatorname{char} k = p > 0$. Take a p-basis B of k over Π, so that Γ_B is linearly independent over $k^p(\Pi) = k^p$. Further, since $\{dx \colon x \in B\}$ is k-linearly independent in Ω_k, according to our hypothesis, these must be K-linearly independnet in Ω_K, as a result, Γ_B is linearly independent over $K^p(\Pi) = K^p$. It follows then from the standard argument that the multiplication map $k \otimes_{k^p} K^p \to k[K^p]$ is injective, therefore, k and K^p are linearly disjoint over k^p. The fact that the Frobenius morphism exists then implies that K and $k^{1/p}$ are linearly disjoint over k. In view of Theorem 2.10, K/k is separable, as desired. ∎

DEFINITION 2.18. Let k be a field of characteristic $p > 0$ with $\Pi \subseteq k$ the prime subfield. An *absolute p-basis* of k is a p-basis of the extension k/Π.

Note that if $k_0 \subseteq k$ is a perfect subfield, then an absolute p-basis of k is also a p-basis for the extension k/k_0.

THEOREM 2.19. Let k be a field of characteristic $p > 0$. If an absolute p-basis of k is also an absolute p-basis of K, then K is 0-étale over k. Conversely, if K is 0-étale over k, then any absolute p-basis of k is an absolute p-basis of K.

Proof. Let C be a k-algebra with an ideal $N \trianglelefteq C$ such that $N^2 = 0$. Set $\overline{C} = C/N$ and consider a commutative diagram of k-algebra homomorphisms:

$$\begin{tikzcd}
k \arrow[r, "j"] \arrow[d, "i"'] & C \arrow[d, "\pi"] \\
K \arrow[r, "u"'] & \overline{C}.
\end{tikzcd}$$

Let B be an absolute p-basis of k which is also an absolute p-basis of K. This would imply that the natural map $\alpha \colon \Omega_k \otimes_k K \to \Omega_K$ is an isomorphism, which, in view of Theorem 2.17 implies that K/k is separable. Further, since Γ_B is also a K^p-basis of K, it follows that $K = K^p[k]$, i.e., the natural multiplication map $K^p \otimes_{k^p} k \to K$ is an isomorphism. We shall use this isomorphism and the universal property of the pushout diagram:

$$\begin{tikzcd}
k^p \arrow[r] \arrow[d] & K^p \arrow[d] \\
k \arrow[r] & K^p \otimes_{k^p} k
\end{tikzcd}$$

to construct a lifting $K \to C$.

Our first goal is to define as k^p-homomorphism $K^p \to C$. For each $\alpha \in K$, choose an $a \in C$ with $\pi(a) = u(\alpha)$, and define $v_0 : K^p \to C$ by $v_0(\alpha^p) = a^p$. We must show that this is independent of the choice of a. Indeed, if $a' \in C$ is such that $\pi(a) = \pi(a') = u(\alpha)$, then $a' = a + x$ for some $x \in N$, and hence,

$$a'^p = a^p + x^p = a^p,$$

since $p \geqslant 2$. Clearly v_0 is a k^p-homomorphism. The pushout of the maps $v_0 : K^p \to C$ and $j : k \to C$ determines a morphism $v : K \to C$ lifting u to C. The uniqueness of this lifting follows from the fact that $K^p[k] = K$.

Conversely, if K/k is 0-étale, then it is 0-unramified so that Lemma 1.8 implies $\Omega_{K/k} = 0$. From 0-smoothness and Theorem 1.9, the map $\alpha : \Omega_k \otimes_k K \to \Omega_K$ is an isomorphism, so that an absolute p-basis of k is also an absolute p-basis of K. This completes the proof. ■

Theorem 2.20. Let K/k be a separable extension of fields of characteristic $p > 0$, and let B be a p-basis of K/k. Then B is algebraically independent over k.

Proof. Suppose not and $b_1, \ldots, b_n \in B$ are algebraically dependent over k. Choose $0 \neq f(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ is a polynomial of minimal degree with $f(b_1, \ldots, b_n) = 0$, and let $d = \deg f$. We can group the monomials of f together and write

$$f(X_1, \ldots, X_n) = \sum_{0 \leqslant i_1, \ldots, i_n < p} g_{i_1, \ldots, i_n}(X_1^p, \ldots, X_n^p) X_1^{i_1} \cdots X_n^{i_n}$$

for some $g_{i_1, \ldots, i_n} \in k[X_1, \ldots, X_n]$. Note that $b_1, \ldots, b_n$ are p-independent over k, and hence, $g_{i_1, \ldots, i_n}(b_1^p, \ldots, b_n^p) = 0$ for all $0 \leqslant i_1, \ldots, i_n < p$. The minimality of $\deg f$ then forces

$$f(X) = g_{0, \ldots, 0}(X_1^p, \ldots, X_n^p) = h(X_1, \ldots, X_n)^p$$

for some $h(X_1, \ldots, X_n) \in k^{1/p}[X_1, \ldots, X_n]$. Note that monomials of degree $< d$ are linearly independent over k, and since K and $k^{1/p}$ are linearly disjoint over k, these monomials must be linearly independent over $k^{1/p}$. Thus $h(b_1, \ldots, b_n) \neq 0$, a contradiction to the fact that $f(b_1, \ldots, b_n) = 0$. Thus B must be algebraically independent over k. ■

Theorem 2.21. If K/k is a separable field extension of a field k, then K is 0-smooth over k. Conversely, if K is 0-smooth over k, then K/k is a separable field extension.

Proof. Let B be a differential basis of K/k. Since this extension is separable, in view of Theorem 2.20 and Theorem 2.13, $k(B)$ is purely transcendental over k. Clearly $k(B)$ is 0-smooth over k due to the universal property of purely transcendental extensions. We contend that $K/k(B)$ is 0-étale. In characteristic 0, this is a consequence of Theorem 1.11. In characteristic $p > 0$, due to Theorem 2.17 and Theorem 1.9, the sequence

$$0 \to \Omega_k \otimes_k K \xrightarrow{\alpha} \Omega_K \xrightarrow{\beta} \Omega_{K/k} \to 0$$

is exact. It follows hence that choosing a differential basis of k/Π and putting it together with B, we obtain a differential basis $\mathfrak{B}$ of Ω_K, that is, an absolute p-basis of K. Note that here we are using the explicit description of the map β. This is clearly an absolute p-basis of $k(B)$, whence $K/k(B)$ is 0-étale due to Theorem 2.19. A standard abstract nonsense argument shows that K/k is 0-smooth.

Conversely, if K/k is 0-smooth, then from Theorem 1.9, the map $\Omega_k \otimes_k K \to \Omega_K$ is injective, so that by Theorem 2.17, K/k is separable. ■

Porism 2.22. If K/k is a separable extension of fields, and B a differntial basis of $\Omega_{K/k}$, then K is 0-étale over $k(B)$.

References

[Sta18] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2018.